



Grant Thornton

An instinct for growth™

## Information Commissioner's Office

---

*Internal Audit 2013-14: Financial management: Debit and credit card payments in ICE*

Last updated 4 February 2014

Distribution		Timetable	
For action	Director of Corporate Services	Fieldwork completed	18 December 2013
	Head of Finance	Draft report issued	8 January 2014
For information	Audit Committee	Management comments	4 February 2014
		Final report issued	4 February 2014

This report is confidential and is intended for use by the management and Directors of the ICO only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of the ICO management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

## Executive Summary

### Background

Under the Data Protection Act 1998, every data controller who is processing personal information is required to register with the ICO. Payments of either £500 or £35 annually are required as a registration fee, based on staff levels and turnover, yielding a combined income to the ICO of approximately £16 million per year.

In May 2013, the ICO went live with its new ICE (ICO Customer Engagement) system. In conjunction with this, online payment of registration fees by debit or credit card was introduced. These currently account for around 25% of monthly fee income, with cheque and BACS payments reducing accordingly.

A project team, led by Operations Service Delivery, have established the process for the transfer of information into ICE from Barclaycard online, the host website for credit and debit card payments. It is this project team who, following requests from the relevant departments, are managing the ongoing implementation progresses.

### Scope

Our review involved an assessment of the following risks:

Finance may not have clearly documented and communicated the controls over the file transfer from Barclays to ICE and journal entries into the finance system, or such controls may not be efficient or applied as intended, which may impact the integrity of credit/debit card payment data;

Controls over staff access to ICE and the ability to amend customer payment information may not be sufficient, resulting in the risk that inappropriate changes could be made to payment information;

Systems may not enable management to identify where an organisation has paid the wrong amount by credit/debit card, resulting in the wrong amounts being collected; and  
Processes and authorisation required to refund payments made by credit or debit card may not be clearly documented or may not be applied, resulting in inappropriate refunds being paid.

Further details on responsibilities, approach and scope are included in Appendix A.

### Overall assessment

We have made an overall assessment of our findings as:

Overall assessment	
We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.	Green

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

### Key findings

Risk / Process	High	Medium	Low	Imp
File transfer from Barclays to ICE	-	-	-	-
Staff access to ICE	-	-	-	-
Identifying incorrect payments and management reporting	-	1	1	-
Credit and debit card refunds	-	-	-	-
<b>Total</b>	-	<b>1</b>	<b>1</b>	-

The following finding was rated as medium priority:

Certain Management Information and data from the ICE system is insufficient for the purposes of financial reporting and to meet the needs of the Finance and Notifications teams. Further, the lack of functionality within ICE has resulted in significant inefficiencies and delays when attempting to reconcile variances between expected payment amounts and the figures actually recorded in ICE.

Further details of our findings and recommendations are provided in Section 2.

### **Basis of preparation**

Whilst we report by exception, we draw attention to the following matters in addition to the issues raised within the findings section of this report.

There is a clearly documented process for completing the daily file transfer from Barclaycard and reconciling the amount taken from Barclaycard and uploaded into ICE, and the figure subsequently received by the bank.

The Finance team operate a daily reconciliation process, to ensure that the total daily payment per Barclaycard reconciles to the amount transferred into ICE and the amount received to the bank account.

The daily file transfer from Barclaycard to ICE updates each individual data controller record for which payment has been made.

Due to the use of Barclaycard online as a host website, no credit or debit card payment details can be manually changed by any member of ICO staff.

Access to amend the payment file prior to upload is restricted to the Finance Officers who download it, and the ability to amend a payment amount once recorded in ICE is restricted to the project team system administrators. Any such changes would be highlighted through the reconciliation process, and as noted in seven such instances during our testing, all were supported by explanatory notes and an audit trail in ICE.

All tier changes (i.e. from £35 to £500 payments and vice versa) and refunds processed by the Notifications team are automatically put into a management queue for approval within ICE, giving review over the accuracy of the payment.

Once approved, credit and debit card refunds are paid directly back to the relevant card on a weekly basis using Barclaycard online, and signed as complete by two members of Finance staff. For a sample of 10 refund batches, we confirmed that all had been signed accordingly. For 10 individual refunds selected from these, we confirmed that the refund had been approved in ICE and subsequently refunded back to cardholder using Barclaycard online.

### **Acknowledgement**

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

## Detailed Findings

### Systems may not enable management to identify where an organisation has paid the wrong amount by credit/debit card, resulting in the wrong amounts being collected

1.	Medium	Reporting capabilities of ICE
Finding and Implication	Proposed action	Agreed action ( <i>Date / Ownership</i> )
<p>Currently, ICE is unable to collate information and analyse data to the extent required by both Finance and Notifications in respect of credit and debit card payments. No information from ICE is used by the Head of Finance to inform operations and support financial reporting. Further, only high level figures are able to be extracted by the Notifications Manager with no detail of individual additions, removals and renewals to the register being available for review or investigation.</p> <p>In addition, the process of reconciling debit and credit card payments can be inefficient. Where variances are highlighted, identifying the specific payment can take significant amounts of time if the variance occurs in ICE, due to the fact information cannot be extracted into Excel and compared to the upload file or the list of payments received.</p> <p>We discussed these issues with management and found that they have been communicated to the ICE project team, however due to the level of updates and amendments required, these are yet to be dealt with.</p> <p>Whilst our review is able to provide assurance that the manual reconciliation processes are operating effectively, the lack of data analysis and management information from ICE gives rise to inefficiencies and time consuming processes, as well as poor management information and a failure to maximise the impact of the investment in ICE.</p>	<p>All ICE functionality issues should be logged with the ICE project team and resolution dates agreed and tracked to the satisfaction of the Finance and Notifications teams.</p>	<p><i>Agreed action</i> The priority for the existing project team resources is to resolve the current ICE performance issues and to implement the web-front end by the end of the financial year. We have prioritised a number of functionality improvements and system enhancements which we are working to implement by the end of the financial year.</p> <p>All functionality issues have been captured through the use of a dedicated email account and logged on the project backlog. An MI reporting workstream has been identified and scoped.</p> <p>It is intended that some progress will have been made by 1 April 2014 however with the current staff resources and priorities it is not practical to commit to a specific output timeline yet.</p> <p><i>Date Effective: Review 1 April 2014</i></p> <p><i>Owner: Paul Lee/David Wells</i></p>

2.	Low	Sample checks of payment amounts
Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>Prior to going live with ICE in May 2013, data controller tier assessments were submitted in paper form allowing for a brief review on processing by Notifications, to identify any registrations which appeared to be for the incorrect amount.</p> <p>Further, sample checks of 20 to 30 registrations per month were undertaken to agree the tier registration paid as being appropriate for that data controller. This helped to confirm that data controllers annually renewing at £35 had not fulfilled the criteria to pay £500, and vice versa.</p> <p>Since the system moved online, there can be no such high level check of paper registrations. Further, monthly sample checks have ceased, due to the volume of work involved in the system transfer and the associated level of outstanding issues the Notifications team have had to resolve as a result of this.</p> <p>The intention for this year is for the NAO (National Audit Office) to complete a sample check as part of their Regularity Audit. 30 will be tested in January 2014, with a final 40 tested in April.</p> <p>The intention is to extend the sample size and undertake further testing should any errors be identified.</p>	<p>The ICO intend to undertake sample checks as part of the NAO Regularity Audit.</p> <p>Given the potential impact on revenues to the ICO, the level of coverage of this control should be approved as suitable by the Executive.</p>	<p><i>Agreed action</i></p> <p>In response to the workload pressures on Notification following the go-live of ICE, the routine regularity testing by the notification team ceased.</p> <p>We have discussed the testing of fee income regularity with the NAO, and our intended approach is to incorporate our testing alongside the NAO sampling.</p> <p>This will be done for the first time as part of the Interim Audit testing at the end of January 2014, and those results will inform the future approach to ensure the ICO is achieving assurance.</p> <p>We hope that a smaller sample will be required in future, given that the larger sampling that has been taking place since the tiered fees were introduced in October 2009 has not suggested any regularity issues.</p> <p>Once the final approach has been determined, approval from the Executive Team will be sought formally.</p> <p><i>Date Effective:</i> Formal approval by 31 March 2014</p> <p><i>Owner:</i> Paul Arnold/Traci Shirley</p>

## Internal audit approach

### Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards (2013) and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005). In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

As part of our 2013-14 Audit Plan, we agreed with the Audit Committee and management that we should carry out a review of the ICO's arrangements for managing credit and debit card payments in ICE, to further inform our ongoing understanding of the ICO's key internal control activities.

Our aim in completing this audit was to ensure that the ICO has appropriate arrangements in place to identify, manage and report on risk.

We achieved our audit objectives by:

Walking through the debit and credit card payments process to gain an understanding of the arrangements in place;

Reviewing key process documents that support the arrangements in place;

Testing a sample of specific processes, including payment reconciliations, refunds and other exceptions identified from credit and debit card payments; and

Reviewing the level of management information available on credit and debit card payments.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

### Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should therefore maintain

sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

## Scope

Our review involved an assessment of the following risks:

Finance may not have clearly documented and communicated the controls over the file transfer from Barclays to ICE and journal entries into the finance system, or such controls may not be efficient or applied as intended, which may impact the integrity of credit/debit card payment data;

Controls over staff access to ICE and the ability to amend customer payment information may not be sufficient, resulting in the risk that inappropriate changes could be made to payment information;

Systems may not enable management to identify where an organisation has paid the wrong amount by credit/debit card, resulting in the wrong amounts being collected; and

Processes and authorisation required to refund payments made by credit or debit card may not be clearly documented or may not be applied, resulting in inappropriate refunds being paid.

## Additional information

### Client staff

The following staff were consulted as part of this review:

Head of Finance  
Finance Officers  
Notifications Manager

### Documents received

The following documents were received during the course of this audit:

Credit and debit card procedures and Finance Manual extracts  
Monthly finance reports and Executive Team minutes  
Monthly finance reconciliation of finance system to bank account  
Monthly bank reconciliations  
Walkthroughs and testing of the daily credit and debit card payments were completed on site, with a sample taken as evidence and stored on the Finance shared drive for data protection reasons

### Locations

The following locations were visited during the course of this review:

The Information Commissioner's Office, Wilmslow

## Overall assessment and audit issues ratings

### Overall assessment

Rating	Description
<b>Red</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
<b>Amber</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
<b>Green</b>	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

### Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features
<b>High</b>	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	<ul style="list-style-type: none"> <li>• Key control not designed or operating effectively</li> <li>• Potential for fraud identified</li> <li>• Non compliance with key procedures / standards</li> <li>• Non compliance with regulation</li> </ul>
<b>Medium</b>	Important findings that are to be resolved by line management.	<ul style="list-style-type: none"> <li>• Impact is contained within the department and compensating controls would detect errors</li> <li>• Possibility for fraud exists</li> <li>• Control failures identified but not in key controls</li> <li>• Non compliance with procedures / standards (but not resulting in key control failure)</li> </ul>
<b>Low</b>	Findings that identify non-compliance with established procedures.	<ul style="list-style-type: none"> <li>• Minor control weakness</li> <li>• Minor non compliance with procedures / standards</li> </ul>
<b>Improvement</b>	Items requiring no action but which may be of interest to management or best practice advice	<ul style="list-style-type: none"> <li>• Information for department management</li> <li>• Control operating but not necessarily in accordance with best practice</li> </ul>





# Grant Thornton

An instinct for growth™

**[www.grant-thornton.co.uk](http://www.grant-thornton.co.uk)**

© 2013 Grant Thornton UK LLP. All rights reserved.

## **Chartered Accountants**

Grant Thornton UK LLP is a limited liability partnership registered in England and Wales: No.OC307742. Registered office: Grant Thornton House, Melton Street, Euston Square, London NW1 2EP.

A list of members is available from our registered office. Grant Thornton UK LLP is authorised and regulated by the Financial Conduct Authority.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.